UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/817,148	04/02/2004	Andrew Dellow	851963.416	1198

38106 7590 11/04/2008

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC
701 FIFTH AVENUE, SUITE 5400
SEATTLE, WA 98104-7092

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
11/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/817,148	DELLOW ET AL.	
	Examiner	Art Unit	
	DEVIN ALMEIDA	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 8/8/2008.

Response to Arguments

Applicant's arguments filed 8/8/2008 have been fully considered but they are not persuasive. Goffin clearly teaches a verifier processor to receive the application code via the internal bus (see figure 1 i.e. memory bus 105), wherein the verifier processor is arranged to continually process the application code using a verification function. See page 11, lines 2-5, i.e., the secure processor also may continually re-authenticate code previously received and stored in a memory unit to prevent unauthorized tampering with. While the processor (master processor 101) executes the application code from the memory independently of the verifier processor (see page 14 lines 17-26 i.e. The operation of the secure processor can be kept from interfering with or slowing the operation of the computing device by requiring the secure processor to access the memory blocks of the memory unit during "stolen" bus cycles. This means that the secure processor is only allowed to access the memory unit during bus cycles for which the master processor is occupied with internal processing and is not accessing the memory bus), and to impair the function of the integrated circuit in the event that the application code does not satisfy the verification function (see page 13 lines 1-14 i.e. If, on the other hand, the authentication signatures do not match, or the data block does not include an authentication signature at all, the secure processor determines that the code has been altered, perhaps to include a virus, during transmission or has been sent by an unauthorized sender who has no authority to reprogram the computing device.

The secure processor can then erase or disable the adulterated memory block or blocks.)

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-4, 14-17, 19, 21, 22, 24, 25, 27, 28, 30-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren (U.S. 6,430,727) in view Goffin (WO 01/61437).

With respect to claim 1, a semiconductor integrated circuit arranged to execute application code to be received from a memory via external connections, comprising:

a processor (see Warren column 2 line 24-47 i.e. CPU) to execute the application code from the memory (see Warren column 2 line 24-47 i.e. memory);

an internal bus (see Warren column 2 line 24-47 i.e. bus) to provide the application code to the processor from the memory (see Warren column 2 line 24-47); and

an instruction monitor to monitor code requests issued by the processor and to impair the function of the circuit unless addresses of the code requests fall within a given range (see Warren abstract and column 2 line 24-47).

Warren does not teach a verifier processor arranged to receive the application code via the internal bus, wherein the verifier processor is arranged to continually process the application code using a verification function whilst the processor executes from the memory and to impair the function of the integrated circuit in the event that the

application code does not satisfy the verification function. Goffin teach Goffin clearly teaches a verifier processor to receive the application code via the internal bus (see figure 1 i.e. memory bus 105), wherein the verifier processor is arranged to continually process the application code using a verification function (see page 11 lines 2-5 i.e. The secure processor also may continually re-authenticate code previously received and stored in a memory unit to prevent unauthorized tampering with) while the processor (master processor 101) executes the application code from the memory independently of the verifier processor (see page 14 lines 17-26 i.e. The operation of the secure processor can be kept from interfering with or slowing the operation of the computing device by requiring the secure processor to access the memory blocks of the memory unit during "stolen" bus cycles. This means that the secure processor is only allowed to access the memory unit during bus cycles for which the master processor is occupied with internal processing and is not accessing the memory bus), and to impair the function of the integrated circuit in the event that the application code does not satisfy the verification function (see page 13 lines 1-14 i.e. If, on the other hand, the authentication signatures do not match, or the data block does not include an authentication signature at all, the secure processor determines that the code has been altered, perhaps to include a virus, during transmission or has been sent by an unauthorized sender who has no authority to reprogram the computing device. The secure processor can then erase or disable the adulterated memory block or blocks.)

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a separate

processor for verifying code to increase the security of the system (see page 10 line 26 – page 13 line 25). Therefore one would have been motivated to have a verifier processor.

With respect to claim 2, wherein the given range is stored in an internal memory (see Warren column 2 line 48-54).

With respect to claim 3, wherein the given range is derived by the verifier processor during a first check of the memory (see Warren column 2 line 24-60).

With respect to claim 4, wherein the application code in memory comprises a linked list and wherein the given range comprises a table of linked list addresses (see Warren column 2 line 24-60).

With respect to claim 14, wherein the verifier processor is to request portions of the application code from the flash memory at intervals between requests by the processor for portions of the application code (see Warren column 2 line 24-60).

With respect to claim 15, wherein the verifier processor is to request portions of the application code at less frequent intervals than the processor (see Warren column 2 line 24-60).

With respect to claim 16, wherein the verifier processor is to request portions of the application code at pseudo random times (see Warren column 2 line 24-60).

With respect to claim 17, wherein the verifier processor is to carry out read requests at a faster rate during a first check than in subsequent checks (see Warren column 2 line 24-60).

With respect to claims 19 and 25, a semiconductor integrated circuit arranged to execute application code received from an external memory via an external connection, comprising: a processor (see Warren column 2 line 24-47 i.e. CPU) to execute the application code from the memory (see Warren column 2 line 24-47 i.e. memory); an internal bus (see Warren column 2 line 24-47 i.e. bus) connected to the processor to provide the application code to the processor from the memory (see Warren column 2 line 24-47); and an instruction monitor to be connected to the internal bus to monitor code requests issued by the processor and to impair the function of the circuit unless the address of the code falls within a given range (see Warren column 2 line 24-47).

Warren does not teach a verifier processor arranged to receive the application code via the internal bus, wherein the verifier processor is arranged to continually process the application code using a verification function whilst the processor executes from the memory and to impair the function of the integrated circuit in the event that the application code does not satisfy the verification function. Goffin teach a verifier processor (security processor 102) arranged to receive the application code via the internal bus (memory bus 105), wherein the verifier processor is arranged to continually process the application code using a verification function while the processor (master processor 101) executes from the memory and to impair the function of the integrated circuit in the event that the application code does not satisfy the verification function (see page 10 line 26 – page 13 line 25).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a separate

processor for verifying code to increase the security of the system (see page 10 line 26 – page 13 line 25). Therefore one would have been motivated to have a verifier processor.

With respect to claims 21 and 27, wherein the given range is derived by the verifier processor during a check of the memory (see Warren column 2 line 24-54).

With respect to claims 22 and 28, wherein the application code in memory comprises a linked list and wherein the given range is stored in a table of linked list addresses (see Warren column 2 line 24-54).

With respect to claims 24 and 30, wherein the verification processor includes: an internal processor (see Warren column 2 line 24-47 i.e. CPU) that coordinates the processing of the application using the verification function and impairs the execution of the integrated circuit if the application code does not satisfy the verification function (see Warren column 2 line 24-54); a code memory, coupled to the internal processor (see Warren column 2 line 24-47 i.e. CPU); and an interface circuit that connects the internal processor with the internal bus (see Warren column 2 line 24-47 i.e. bus).

With respect to claim 31, a method for executing application code received from an external memory via external connections, the method comprising: executing application code from the external memory (see Goffin figure 1 External data line 106) with a processor (see Goffin figure 1 Master Processor 101 and page 10 line 3 – page 13 line 25); providing the application code to the processor via an internal bus (see Goffin page 10 line 3 – page 13 line 25); providing the application code to a verifier processor via the internal bus (see Goffin figure 1 Secure Processor 102 and page 10

line 3 – page 13 line 25); continually processing the application code with the verifier processor, while the processor executes the application code independently of the verifier processor, using a verification function (see Goffin page 10 line 3 – page 13 line 25); monitoring code requests issued by the processor with an instruction monitor (see Goffin page 10 line 3 – page 13 line 25); and impairing operation of the integrated circuit if the application code does not satisfy the verification function or if addresses of the code requests fall outside a given range (see Goffin page 10 line 3 – page 13 line 25).

With respect to claim 32, further comprising deriving the given range with the verifier processor during a check of the external memory (see Warren column 2 line 24-60).

With respect to claim 33, further comprising storing the given range in an internal memory (see Warren abstract and column 2 line 24-47).

With respect to claim 34, further comprising: receiving pause and stop requests at the verifier processor; and configuring the verifier processor so that any pause and stop request is ineffective during a first check of the code (see Warren column 2 line 24-60).

Claims 10-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren (U.S. 6,430,727) in view Goffin (WO 01/61437) in further view of Morais (U.S. 2003/0229777).

Warren and Goffin teach everthing with respect to claim 1 above but with respect to claim 10 they do not teach wherein the verification function includes a hash function

on the application code. Morais teaches wherein the verification function includes a hash function on the application code (see Morais figure 4 and paragraph 0034-0039 i.e. The comparison is made in a decision step 256 to determine if the stored hash value is equal to the actual hash value that was determined. If not, the machine instructions in bootstrap code implement a step 258, which stops the boot-up process of game console).

It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have included a hash function on the application code to compared to a stored hash value that is maintained in a circuit component of the electronic device, separate from the memory where the code is stored, to verify that the predefined portion of the code is authorized. If the first hash value equals the stored hash value, execution of the predefined portion of the code is enabled, and if not, the boot-up of the electronic device is terminated (see paragraph 0009). Therefore one would have been motivated to have included a hash function on the application code

With respect to claim 11, wherein the verifier processor is arranged to receive a stored secret from the memory and the verification function is a comparison of the secret and the processed application code (see Morais figure 4 and paragraph 0034-0039 i.e. The comparison is made in a decision step 256 to determine if the stored hash value is equal to the actual hash value that was determined. If not, the machine instructions in bootstrap code implement a step 258, which stops the boot-up process of game console).

With respect to claim 12, wherein the verification function comprises hashing the application code to produce hashed code, retrieving a signature of the code from a signature store within the memory and verifying the hashed code and signature using a public key (see Morais figure 4 step 266).

Claims 5-9, 13, 18, 23 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Warren (U.S. 6,430,727) in view Goffin (WO 01/61437) of Harding et al (U.S. 2003/0005277).

Warren and Goffin teach everything with respect to claim 4 above but with respect to claim 5, they do not teach wherein the verifier processor is arranged to impair the function of the integrated circuit if the verification function is not completed for one complete cycle of the linked list within a predetermined time (see Harding paragraph 0016). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a timer to make sure the BIOS has finished in a certain amount of time to make sure that the BIOS is going as planned (see Harding paragraph 0016). Therefore one would have been motivated to have included a timer.

With respect to claim 6, wherein the verifier processor is arranged to receive pause and stop requests and is configured so that any pause and stop request is ineffective during a first check of the code (see Harding paragraph 0016).

With respect to claim 7, wherein the verifier processor can only be paused for a predetermined time (see Harding paragraph 0016).

With respect to claim 8, wherein if the application codes does not satisfy the verification function, a reset signal is asserted after a predetermined time (see Harding paragraph 0016 i.e. this may restart the validation).

With respect to claim 9, wherein a status signal is set and stored to indicate that the code does not satisfy the verification function before the reset is asserted (see Harding paragraph 0016 0018 and 0020).

With respect to claim 13, wherein the verifier processor has a stop input and is arranged to restart a given time period after a stop, and arranged not to stop again until completing the verification function on the code at least once (see Harding paragraph 0016).

With respect to claim 18, wherein impairing the function of the integrated circuit comprises resetting the circuit (see Harding paragraph 0016 i.e. this may restart the validation).

With respect to claims 23 and 29, wherein the verification processor is structured to impair the execution of the circuit by asserting a reset signal to the processor if the application codes does not satisfy the verification function (see Morais paragraph 0034-0039) within a predetermined time (see Harding paragraph 0016).

Conclusion

1. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Devin Almeida/
Patent Examiner, Art Unit 2432

10/28/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432